CLAIMS

1. A method of obtaining secure registration by a memory module (UICC) in a multicast-broadcast-multimedia system (MBMS), the method comprising:

receiving a random number;

generating a radio access network key (RAK) as a function of the random number and a key selected from the group consisting of a public land mobile network key (PK) and a broadcast access key (BAK); and

generating a temporary registration key (RGK) as a function of the RAK.

- 2. The method of claim 1, further comprising transmitting the RGK to a mobile telephone.
- 3. The method of claim 1, further comprising receiving a provisioning message from a broadcast-multicast service center.
- 4. The method of claim 3, wherein the provisioning message is a function of the PK and a permanent registration key (RK).

- 5. The method of claim 3, further comprising extracting the PK from the provisioning message.
- 6. The method of claim 1, wherein the RGK is a function of the RAK, a service identification number and a user identification number.
- 7. The method of claim 6, wherein the RGK is a function of the RAK and a cyclic redundancy code (CRC) computed from the service identification number and the user identification number.
- 8. The method of claim 1, wherein the UICC comprises a subscriber identity module (SIM) in a Global System for Mobile communication (GSM) system.
- 9. The method of claim 1, wherein the UICC comprises a removable user identity module (RUIM) in a code division multiple access (CDMA) system.
- 10. The method of claim 1, wherein the PK is provisioned by using a public key.
- 11. The method of claim 1, wherein the BAK is provisioned by using a public key.

12. A method of obtaining secure registration by a mobile station in a multicast-broadcast-multimedia system (MBMS), the method comprising:

receiving a random number from a radio access network;

transmitting the random number to a memory module (UICC); and

receiving from the UICC a temporary registration key (RGK) based on the random number.

- 13. The method of claim 12, wherein the RGK is a function of a radio access network key (RAK) which is a function of the random number and a key selected from the group consisting of a public land mobile network key (PK) and a broadcast access key (BAK).
- 14. The method of claim 13, wherein the PK is extracted from a provisioning message received from a broadcast-multicast service center.
- 15. The method of claim 14, wherein the provisioning message is a function of the PK and a permanent registration key (RK).

- 16. The method of claim 13, wherein the RGK is a function of the RAK, a service identification number and a user identification number.
- 17. The method of claim 16, wherein the RGK is a function of the RAK and a cyclic redundancy code (CRC) computed from the service identification number and the user identification number.
- 18. The method of claim 12, wherein the UICC comprises a subscriber identity module (SIM) in a Global System for Mobile communication (GSM) system.
- 19. The method of claim 12, wherein the UICC comprises a removable user identity module (RUIM) in a code division multiple access (CDMA) system.
- 20. The method of claim 12, wherein the PK is provisioned by using a public key.
- 21. The method of claim 12, wherein the BAK is provisioned by using a public key.
 - 22. A memory module, comprising:
 means for receiving a random number;

means for generating a radio access network key

(RAK) as a function of the random number and a key selected

from the group consisting of a public land mobile network

key (PK) and a broadcast access key (BAK); and

means for generating a temporary registration key (RGK) as a function of the RAK.

- 23. The memory module of claim 22, further comprising means for transmitting the RGK to a mobile telephone.
- 24. The memory module of claim 22, further comprising means for receiving a provisioning message from a broadcast-multicast service center.
- 25. The memory module of claim 24, wherein the provisioning message is a function of the PK and a permanent registration key (RK).
- 26. The memory module of claim 24, further comprising means for extracting the PK from the provisioning message.
- 27. The memory module of claim 22, wherein the RGK is a function of the RAK, a service identification number and a user identification number.

- 28. The memory module of claim 27, wherein the RGK is a function of the RAK and a cyclic redundancy code (CRC) computed from the service identification number and the user identification number.
- 29. The memory module of claim 22, wherein the PK is provisioned by using a public key.
- 30. The memory module of claim 22, wherein the BAK is provisioned by using a public key.
 - 31. A mobile station apparatus, comprising:

means for receiving a random number from a radio access network;

means for transmitting the random number to a memory module (UICC); and

means for receiving from the UICC a temporary registration key (RGK) based on the random number.

32. The apparatus of claim 31, wherein the RGK is a function of a radio access network key (RAK) which is a function of the random number and a key selected from the group consisting of a public land mobile network key (PK) and a broadcast access key (BAK).

- 33. The apparatus of claim 32, wherein the PK is extracted from a provisioning message received from a broadcast-multicast service center.
- 34. The apparatus of claim 33, wherein the provisioning message is a function of the PK and a permanent registration key (RK).
- 35. The apparatus of claim 32, wherein the RGK is a function of the RAK, a service identification number and a user identification number.
- 36. The apparatus of claim 35, wherein the RGK is a function of the RAK and a cyclic redundancy code (CRC) computed from the service identification number and the user identification number.
- 37. The apparatus of claim 31, wherein the UICC comprises a subscriber identity module (SIM) in a Global System for Mobile communication (GSM) system.
- 38. The apparatus of claim 31, wherein the UICC comprises a removable user identity module (RUIM) in a code division multiple access (CDMA) system.

- 39. The apparatus of claim 31, wherein the PK is provisioned by using a public key.
- 40. The apparatus of claim 31, wherein the BAK is provisioned by using a public key.
- 41. A computer readable medium embodying a method of obtaining secure registration by a memory module (UICC) in a multicast-broadcast-multimedia system (MBMS), the method comprising:

receiving a random number;

generating a radio access network key (RAK) as a function of the random number and a key selected from the group consisting of a public land mobile network key (PK) and a broadcast access key (BAK); and

generating a temporary registration key (RGK) as a function of the RAK.

- 42. The computer readable medium of claim 41, wherein the method further comprises transmitting the RGK to a mobile telephone.
- 43. The computer readable medium of claim 41, wherein the method further comprises receiving a provisioning message from a broadcast-multicast service center.

- 44. The computer readable medium of claim 43, wherein the provisioning message is a function of the PK and a permanent registration key (RK).
- 45. The computer readable medium of claim 43, wherein the method further comprises extracting the PK from the provisioning message.
- 46. The computer readable medium of claim 41, wherein the RGK is a function of the RAK, a service identification number and a user identification number.
- 47. The computer readable medium of claim 46, wherein the RGK is a function of the RAK and a cyclic redundancy code (CRC) computed from the service identification number and the user identification number.
- 48. The computer readable medium of claim 41, wherein the UICC comprises a subscriber identity module (SIM) in a Global System for Mobile communication (GSM) system.
- 49. The computer readable medium of claim 41, wherein the UICC comprises a removable user identity module (RUIM) in a code division multiple access (CDMA) system.

- 50. The computer readable medium of claim 41, wherein the PK is provisioned by using a public key.
- 51. The computer readable medium of claim 41, wherein the BAK is provisioned by using a public key.
- 52. A computer readable medium embodying a method of obtaining secure registration by a mobile station in a multicast-broadcast-multimedia system (MBMS), the method comprising:

receiving a random number from a radio access network;

transmitting the random number to a memory module (UICC); and

receiving from the UICC a temporary registration key (RGK) based on the random number.

- 53. The computer readable medium of claim 52, wherein the RGK is a function of a radio access network key (RAK) which is a function of the random number and a key selected from the group consisting of a public land mobile network key (PK) and a broadcast access key (BAK).
- 54. The computer readable medium of claim 53, wherein the PK is extracted from a provisioning message received from a broadcast-multicast service center.

- 55. The computer readable medium of claim 54, wherein the provisioning message is a function of the PK and a permanent registration key (RK).
- 56. The computer readable medium of claim 53, wherein the RGK is a function of the RAK, a service identification number and a user identification number.
- 57. The computer readable medium of claim 56, wherein the RGK is a function of the RAK and a cyclic redundancy code (CRC) computed from the service identification number and the user identification number.
- 58. The computer readable medium of claim 52, wherein the UICC comprises a subscriber identity module (SIM) in a Global System for Mobile communication (GSM) system.
- 59. The computer readable medium of claim 52, wherein the UICC comprises a removable user identity module (RUIM) in a code division multiple access (CDMA) system.
- 60. The computer readable medium of claim 52, wherein the PK is provisioned by using a public key.

61. The computer readable medium of claim 52, wherein the BAK is provisioned by using a public key.